



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO.                 | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO.       |
|---------------------------------|-------------|----------------------|---------------------|------------------------|
| 10/612,706                      | 07/02/2003  | Jari Mononen         | P3068US00           | 3738                   |
| 30671                           | 7590        | 01/06/2011           | EXAMINER            |                        |
| DITTHAVONG MORI & STEINER, P.C. |             |                      |                     | BIAGINI, CHRISTOPHER D |
| 918 Prince Street               |             | ART UNIT             |                     | PAPER NUMBER           |
| Alexandria, VA 22314            |             | 2445                 |                     |                        |
|                                 |             |                      | NOTIFICATION DATE   | DELIVERY MODE          |
|                                 |             |                      | 01/06/2011          | ELECTRONIC             |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docket@dcpatent.com

|                              |                        |                     |
|------------------------------|------------------------|---------------------|
| <b>Office Action Summary</b> | <b>Application No.</b> | <b>Applicant(s)</b> |
|                              | 10/612,706             | MONONEN ET AL.      |
|                              | <b>Examiner</b>        | <b>Art Unit</b>     |
|                              | CHRISTOPHER D. BIAGINI | 2445                |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 11/15/2010.

2a) This action is **FINAL**.                    2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 27,31,34-41,45,54-56 and 59-70 is/are pending in the application.

4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.

5) Claim(s) \_\_\_\_\_ is/are allowed.

6) Claim(s) 27, 31, 34-41, 45, 54-56, and 59-70 is/are rejected.

7) Claim(s) \_\_\_\_\_ is/are objected to.

8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All    b) Some \* c) None of:

- Certified copies of the priority documents have been received.
- Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
- Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

|  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                         | Paper No(s)/Mail Date. _____ .                                    |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ . | 5) <input type="checkbox"/> Notice of Informal Patent Application |
|  | 6) <input type="checkbox"/> Other: _____ .                        |

## **DETAILED ACTION**

This communication is responsive to the amendment filed November 15, 2010. Claims 27, 31, 34-39, 41, 45, 54, 55, and 59-70 were amended. Claims 27, 31, 34-41, 45, 54-56, and 59-70 are pending.

### **Response to Arguments**

Applicant's arguments with respect to the specification objections and corresponding rejections under 35 USC 112, first paragraph have been fully considered but are not persuasive.

With respect to claims 27, 34, and 41, Applicant argues that the claims find support in paragraphs [0049], [0052], [0053], and [0078] of the specification as published. The Examiner respectfully disagrees. Indeed, these very paragraphs were identified as being insufficient in the last Office Action. Again, there is absolutely no indication that the security credentials are accessed via the CGI. Applicant presents the last sentence of paragraph [0078] in boldface type, presumably in an attempt to draw attention to the fact that data from “remote devices” can be provided via the CGI. However, the Examiner respectfully submits that, as explained in the last Office Action, there is nothing which indicates that this data is the security credential data mentioned elsewhere. Should Applicant decide to continue seeking the claimed subject matter in its present form, the Examiner respectfully requests that Applicant clearly and explicitly explain how these seemingly incongruent sections of the specification provide support for the claimed combination of features.

With respect to claims 35, 59, and 65, Applicant points to paragraphs [0072] and [0076]. However, there is nothing in these paragraphs which indicates that the security credentials are accessible via a browser. Notably, the paragraphs do not even mention the security credentials.

With respect to claims 36, 60, and 66, Applicant points to paragraphs [0072] and [0073]. However, there is nothing in these paragraphs which indicates that the security challenge is in HTTP and is embedded with a pathname of the CGI. Notably, these paragraphs do not even mention the a security challenge being in HTTP and embedded with the pathname of the CGI.

With respect to claims 37, 61, and 67, Applicant points to paragraphs [0058], [0059], and [0076]. Notably, nowhere do these paragraphs indicate that the security credentials are a live image. Instead, the credentials are a saved image (i.e., not live).

With respect to claims 39, 40, 62, and 68, Applicant points to paragraph [0091] as providing support for the claimed features. Notably, however, these paragraphs do not indicate that the device performs a protocol translation between "the targeted device" (i.e., the one which receives security credentials) and a CGI, much less where that translation is between "a short range communication protocol and a wireless access protocol."

With respect to claims 54, 56, 63, and 69, Applicant points to paragraphs [0050] and [0054] as providing support for the claimed features. Notably, however, these paragraphs do not indicate that the download of the shopping list is performed via the CGI or automatically.

For the reasons given above, Applicant's arguments cannot be held as persuasive.

Applicant's arguments with respect to the rejections under 35 USC 103(a) have been fully considered but are not persuasive. Applicant argues in substance that Nielsen, White, and Hase fail to teach or suggest the subject matter of the independent claims.

First, Applicant argues that there is no reason to combine Nielsen and White. The Examiner respectfully disagrees. In fact, there are numerous reasons. For example, White indicates that CGI applications increase security, as they can be stored in a secure directory tree to which access may be limited. One of ordinary skill would have recognized the benefits of this increased security, such as preventing access by malicious users who seek to do the system harm. Furthermore, as is known in the art and as recognized by White (see col. 6, lines 12-25) indicates that CGI applications are standardized and versatile. One of ordinary skill would have recognized, then, that employing CGIs would decrease the time needed to implement the system, since developers would likely be already familiar with their standardized interface and programming model.

Next, Applicant argues that the combination does not teach or suggest "determining whether an information request includes a reference to a common gateway interface." The Examiner respectfully disagrees. White, for example, indicates that "Sending information to a web server to be processed by a CGI application typically requires the use of an HTML document known as a 'form,'" "the web server executes the CGI application specified in the HTML form," and "the requested CGI application continues execution and processing results are transmitted back to the client" (see col. 6, lines 28-63). Furthermore, White indicates that the server has multiple CGIs (see col. 7, lines 43-47). Thus, White determines whether an information request includes a reference to a common gateway interface (specifically, whether

the request contains a reference to a requested one of the multiple CGIs, as opposed to another one of the multiple CGIs).

## **Specification**

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Specifically, the specification lacks antecedent basis for the following limitations:

- “determine to make security credentials of a user of the mobile terminal accessible for a targeted one of the connected proximate devices via the common gateway interface for verifying user security access” as recited in claims 27, 34, and 41;
- “determining to transfer a uniform resource locator or internet protocol address of the mobile terminal to the targeted device for making the security credentials accessible via a browser” as recited in claims 35, 59, and 65;
- “the security challenge being in HTTP and embedded with a pathname of the common gateway interface” as recited in claims 36, 60, and 66;
- “take a live image of the user of the mobile terminal as the security credentials” as recited in claims 37, 61, and 67;
- “perform a protocol translation between the targeted device and the common gateway interface, and wherein the translation occurs between a short range communication protocol and a wireless access protocol” as recited in claims 39, 40, 62, and 68;

- “automatically download the item list and format a shopping list via the common gateway interface” as recited in claims 54, 56, 63, and 69.

Correction of the above is **required**.

### **Claim Rejections - 35 USC § 112**

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 27, 31, 34-41, 45, 54-56, and 59-70 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claims 27, 34, and 41 recite the limitation “determine to make security credentials of a user of the mobile terminal accessible for a targeted one of the connected proximate devices via the common gateway interface for verifying user security access” (or a similar limitation). Of the sections of the specification identified by the Applicant as providing support for the amendments, the most relevant portion appears to be at paragraphs [0049]-[0053] of the application as published. Notably, neither these paragraphs, nor any other section of the specification, indicate that the user’s security credentials are accessed via a CGI. Moreover, the specification indicates that data local to the mobile terminal (such as the stored biometric

authentication data) are not accessed via the CGI. Paragraph [0078] states "if the information requested is locally accessible...then the information is accessed from server directory 708." As can be seen in Fig. 7, access to server directory 708 is not made through the CGI.

Claims 35, 59, and 65 recite "making the security credentials accessible via a browser." Of the sections of the specification identified by the Applicant as providing support for the amendments, the most relevant portion appears to be at paragraph [0053] of the application as published. This section describes that the credentials may be retrieved via HTTP, but this does mean that they are "accessible via a browser."

Additionally, claims 59 and 65 require that the mobile device transfers the address to the targeted device. Notably, neither this paragraph, nor any other section of the specification, indicates that the mobile terminal transfers the address. In fact, it is disclosed that the user enters a PIN corresponding to the address into a keypad of the security access control point, which then obtains the address from database 310. Database 310 is clearly not part of the mobile terminal (see Fig. 3).

Claims 36, 60, and 66 require that the security challenge is "embedded with a pathname of the common gateway interface." Again, nowhere does the specification indicate that the security challenge passes through the CGI at all, much less by way of a security challenge embedded with a pathname.

Claims 37, 61, and 67 require capturing a “live image...as the security credentials.” Of the sections of the specification identified by the Applicant as providing support for the amendments, the most relevant portion appears to be at paragraph [0051] of the application as published. Notably, neither this paragraph, nor any other section of the specification, indicates that the credentials are a live image. Instead, the credentials are a saved image (i.e., not live).

Claims 39-40, 62, and 68 require that the device perform a protocol translation “between the targeted device” and the CGI, and that the translation is between “a short range communication protocol and a wireless access protocol.” However, nowhere does the specification indicate that the device performs a protocol translation between “the targeted device” (i.e., the one which receives security credentials) and a CGI, much less where that translation is between “a short range communication protocol and a wireless access protocol.”

Claims 54, 56, 63, and 69 recite the limitation “automatically download the item list and format a shopping list via the common gateway interface” (or a similar limitation). Of the sections of the specification identified by the Applicant as providing support for the amendments, the most relevant portion appears to be at paragraph [0054] of the application as published. Notably, however, nowhere does the specification indicate that the download is performed “via” a CGI or “automatically.”

Any claim not specifically addressed above is rejected for at least incorporating the deficiencies of a parent claim.

### **Claim Rejections - 35 USC § 103**

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**Claims 27, 34, and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nielsen (US Pub. No. 2002/0180582) in view of White (US Patent No. 6,049,877).**

Regarding claim 27, Nielsen shows an apparatus comprising:

- at least one processor (inherently disclosed as a necessary component of a mobile phone or handheld computer which functions as an electronic key device: see [0119]); and
- at least one memory including computer program code for one or more programs (inherently disclosed as a necessary component of a mobile phone or handheld computer which functions as an electronic key device: see [0119]),
- the at least one memory and the computer program code configured to, with the at least one processor, cause the apparatus to perform at least the following,
  - determine to connect to one or more proximate external devices (lock control unit 621, which is connected via Bluetooth: see Fig. 2b and [0167]-[0168]), the apparatus functioning as a mobile server (comprising a

device which transfers an access code upon being contacted by the lock control unit: see steps 677 and 688 in Fig. 6c and [0168]); and

- determine to make security credentials of a user of the mobile terminal accessible for a targeted one of the wirelessly connected proximate devices for verifying user security access (comprising providing an access code which permits access to a locked area: see [0113] and [0167]-[0168]),
- wherein the apparatus is a mobile terminal (comprising a mobile phone or handheld computer: see [0119]).

Nielsen does not explicitly show determining whether an information request includes a reference to a common gateway interface, and that the security credentials are made available via the common gateway interface.

White shows determining whether an information request (comprising an HTML form) includes a reference to a common gateway interface (comprising determining whether the request contains a reference to a requested one of multiple CGIs, as opposed to another one of the multiple CGIs: see col. 6, lines 28-63 and col. 7, lines 43-47) and making security credentials available via the common gateway interface (see col. 7, lines 19-25 and col. 7, line 60 to col. 8, line 5).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Nielsen to use a CGI as taught by White in order to improve security, as CGI applications can be stored within a secure directory tree to which access may be limited (see White, col. 1, lines 50-53).

Regarding claim 34, Nielsen shows a method comprising:

- determining to connect between a mobile terminal (an electronic key device: see [0119]) and one or more proximate external devices (lock control unit 621, which is connected via Bluetooth: see Fig. 2b and [0167]-[0168]) that are external to the mobile terminal functioning as a mobile server (comprising a device which transfers an access code upon being contacted by the lock control unit: see steps 677 and 688 in Fig. 6c and [0168]); and
- determining to make security credentials of a user of the mobile terminal accessible for a targeted one of the wirelessly connected proximate devices for verifying user security access (comprising providing an access code which permits access to a locked area: see [0113] and [0167]-[0168]).

Nielsen does not explicitly show determining whether an information request includes a reference to a common gateway interface, and that the security credentials are made available via the common gateway interface.

White shows determining whether an information request (comprising an HTML form) includes a reference to a common gateway interface (comprising determining whether the request contains a reference to a requested one of multiple CGIs, as opposed to another one of the multiple CGIs: see col. 6, lines 28-63 and col. 7, lines 43-47) and making security credentials available via the common gateway interface (see col. 7, lines 19-25 and col. 7, line 60 to col. 8, line 5).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Nielsen to use a CGI as taught by White in order to improve security, as CGI applications can be stored within a secure directory tree to which access may be limited (see White, col. 1, lines 50-53).

Regarding claim 41, Nielsen shows a computer-readable storage medium carrying one or more sequences of one or more instructions (inherently disclosed as a necessary component of a mobile phone or handheld computer which functions as an electronic key device: see [0119]) which, when executed by one or more processors, cause an apparatus to perform the following steps:

- determining to connect to one or more proximate external devices (lock control unit 621, which is connected via Bluetooth: see Fig. 2b and [0167]-[0168]), the apparatus functioning as a mobile server (comprising a device which transfers an access code upon being contacted by the lock control unit: see steps 677 and 688 in Fig. 6c and [0168]); and
- determining to make security credentials of a user of the mobile terminal accessible for a targeted one of the wirelessly connected proximate devices for verifying user security access (comprising providing an access code which permits access to a locked area: see [0113] and [0167]-[0168]),
- wherein the apparatus is a mobile terminal (comprising a mobile phone or handheld computer: see [0119]).

Nielsen does not explicitly show determining whether an information request includes a reference to a common gateway interface, and that the security credentials are made available via the common gateway interface.

White shows determining whether an information request (comprising an HTML form) includes a reference to a common gateway interface (comprising determining whether the request contains a reference to a requested one of multiple CGIs, as opposed to another one of the multiple CGIs: see col. 6, lines 28-63 and col. 7, lines 43-47) and making security credentials available via the common gateway interface (see col. 7, lines 19-25 and col. 7, line 60 to col. 8, line 5).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Nielsen to use a CGI as taught by White in order to improve security, as CGI applications can be stored within a secure directory tree to which access may be limited (see White, col. 1, lines 50-53).

**Claims 31, 38, and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nielsen (US Pub. No. 2002/0180582) in view of White (US Patent No. 6,049,877), and further in view of “Lesson 5: SOAP, UDDI and WSDL” (hereinafter “the Component X Studio Tutorial”).**

Regarding claim 31, the combination further shows determining to respond via the common gateway interface based on an interpretation of the request parameter (see White, col. 8, lines 1-5), but does not show wherein the processor further causes the apparatus to: determine to

facilitate discovery of services offered by the mobile server via a registry of services; determine a request parameter contained in the information request that facilitates correct response interpretation.

The Component X Studio Tutorial shows facilitating discovery of services offered by a server via a registry of services (comprising making the services known via a UDDI registry: see section 5.3 on p. 3) and determining a request parameter contained in the information request that facilitates correct response interpretation (comprising examining a SOAP envelope in a SOAP request which is made according to a WSDL file: see discussion of SOAP at top of p. 2 and discussion of WSDL at pages 3-5).

It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the combination with the discovery facilitation and determining of request parameters taught by the Component X Studio Tutorial in order to provide for a standardized, developer-friendly way to communicate with the server.

Regarding claim 38, the combination further shows determining to respond via the common gateway interface based on an interpretation of the request parameter (see White, col. 8, lines 1-5), but does not show wherein the processor further causes the apparatus to: determining to facilitate discovery of services offered by the mobile server via a registry of services; determine a request parameter contained in the information request that facilitates correct response interpretation.

The Component X Studio Tutorial shows facilitating discovery of services offered by a server via a registry of services (comprising making the services known via a UDDI registry: see

section 5.3 on p. 3) and determining a request parameter contained in the information request that facilitates correct response interpretation (comprising examining a SOAP envelope in a SOAP request which is made according to a WSDL file: see discussion of SOAP at top of p. 2 and discussion of WSDL at pages 3-5).

It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the combination with the discovery facilitation and determining of request parameters taught by the Component X Studio Tutorial in order to provide for a standardized, developer-friendly way to communicate with the server.

Regarding claim 45, the combination further shows determining to respond via the common gateway interface based on an interpretation of the request parameter (see White, col. 8, lines 1-5), but does not show wherein the processor further causes the apparatus to: facilitate discovery of services offered by the mobile server via a registry of services; determine a request parameter contained in the information request that facilitates correct response interpretation.

The Component X Studio Tutorial shows facilitating discovery of services offered by a server via a registry of services (comprising making the services known via a UDDI registry: see section 5.3 on p. 3) and determining a request parameter contained in the information request that facilitates correct response interpretation (comprising examining a SOAP envelope in a SOAP request which is made according to a WSDL file: see discussion of SOAP at top of p. 2 and discussion of WSDL at pages 3-5).

It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the combination with the discovery facilitation and determining of request

parameters taught by the Component X Studio Tutorial in order to provide for a standardized, developer-friendly way to communicate with the server.

**Claims 35, 59, and 65 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nielsen (US Pub. No. 2002/0180582) in view of White (US Patent No. 6,049,877), and further in view of “Understanding Universal Plug and Play”.**

Regarding claim 35, the combination further shows making the security credentials accessible via a browser (see White, col. 8, lines 1-14), but does not explicitly show determining to transferr an uniform resource locator or internet protocol address of the mobile terminal to the targeted device.

Understanding Universal Plug and Play shows transferring a uniform resource locator or internet protocol address to a device (see discussion of “Description” and “Control” on p. 19). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Nielsen in view of White with the address transfer taught by UPnP in order to reduce the amount of configuration that must be performed by users or administrators.

Regarding claim 59, the combination further shows making the security credentials accessible via a browser (see White, col. 8, lines 1-14), but does not explicitly show determining to transfer an uniform resource locator or internet protocol address of the mobile terminal to the targeted device.

Understanding Universal Plug and Play shows transferring a uniform resource locator or internet protocol address to a device (see discussion of “Description” and “Control” on p. 19). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Nielsen in view of White with the address transfer taught by UPnP in order to reduce the amount of configuration that must be performed by users or administrators.

Regarding claim 65, the combination further shows making the security credentials accessible via a browser (see White, col. 8, lines 1-14), but does not explicitly show determining to transfer a uniform resource locator or internet protocol address of the mobile terminal to the targeted device.

Understanding Universal Plug and Play shows transferring a uniform resource locator or internet protocol address to a device (see discussion of “Description” and “Control” on p. 19). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Nielsen in view of White with the address transfer taught by UPnP in order to reduce the amount of configuration that must be performed by users or administrators.

**Claims 36, 60, and 66 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nielsen (US Pub. No. 2002/0180582) in view of White (US Patent No. 6,049,877), and further in view of “Understanding Universal Plug and Play,” Hase (US Pub. No. 2002/0183078), and Urien (US Pub. No. 2002/0124092).**

Regarding claim 36, the combination further shows determining to discover the targeted device by the mobile terminal (see UPnP, p. 18) and transmitting information via HTTP (see White, col. 1, lines 57-59).

The combination does not explicitly receiving a security challenge from the targeted device. Hase shows receiving a security challenge (see [0039]-[0042]). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system to use a security challenge as taught by Hase in order to simplify the timing of when to send credential information.

The combination does not explicitly show that the security challenge is embedded with a pathname of the CGI. Urien shows embedding requests with a pathname of a CGI (see [0153]-[0155]). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system to embed requests with a pathname of a CGI as taught by Urien in order to ensure that the server knows which functionality it should access in response to the request.

Regarding claim 60, the combination further shows determining to discover the targeted device by the mobile terminal (see UPnP, p. 18) and transmitting information via HTTP (see White, col. 1, lines 57-59).

The combination does not explicitly receiving a security challenge from the targeted device. Hase shows receiving a security challenge (see [0039]-[0042]). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the

system to use a security challenge as taught by Hase in order to simplify the timing of when to send credential information.

The combination does not explicitly show that the security challenge is embedded with a pathname of the CGI. Urien shows embedding requests with a pathname of a CGI (see [0153]-[0155]). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system to embed requests with a pathname of a CGI as taught by Urien in order to ensure that the server knows which functionality it should access in response to the request.

Regarding claim 60, the combination further shows determining to discover the targeted device by the mobile terminal (see UPnP, p. 18) and transmitting information via HTTP (see White, col. 1, lines 57-59).

The combination does not explicitly receiving a security challenge from the targeted device. Hase shows receiving a security challenge (see [0039]-[0042]). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system to use a security challenge as taught by Hase in order to simplify the timing of when to send credential information.

The combination does not explicitly show that the security challenge is embedded with a pathname of the CGI. Urien shows embedding requests with a pathname of a CGI (see [0153]-[0155]). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system to embed requests with a pathname of a CGI as taught by Urien in

order to ensure that the server knows which functionality it should access in response to the request.

**Claims 37, 61, and 67 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nielsen (US Pub. No. 2002/0180582) in view of White (US Patent No. 6,049,877), and further in view of Khan (US Pub. No. 2003/0115474).**

Regarding claim 37, the combination does not explicitly show causing the taking of a live image of the user by the mobile terminal as the security credentials for verifying user security access based on facial features.

Khan shows taking a live image as security credentials for verifying user security access based on facial features (see [0008] and [00029]). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system with the biometric identification of Khan in order to provide for improved security.

Regarding claim 61, the combination does not explicitly show causing the taking of a live image of the user by the mobile terminal as the security credentials for verifying user security access based on facial features.

Khan shows taking a live image as security credentials for verifying user security access based on facial features (see [0008] and [00029]). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system with the biometric identification of Khan in order to provide for improved security.

Regarding claim 67, the combination does not explicitly show causing the taking of a live image of the user by the mobile terminal as the security credentials for verifying user security access based on facial features.

Khan shows taking a live image as security credentials for verifying user security access based on facial features (see [0008] and [00029]). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system with the biometric identification of Khan in order to provide for improved security.

**Claims 39, 40, 62, and 68 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nielsen (US Pub. No. 2002/0180582) in view of White (US Patent No. 6,049,877), and further in view of Marchand (WO 0176154).**

Regarding claim 39, the combination does not explicitly show performing a protocol translation between the targeted device and the common gateway interface.

Marchand shows performing a protocol translation (see p. 7, lines 8-25). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the combination with the protocol translation taught by Marchand in order to improve the variety of protocols with which the devices can communicate.

Regarding claim 40, the combination further shows wherein the translation occurs between a short range communication protocol and a wireless access protocol (see Marchand, p. 7, lines 8-25).

Regarding claim 62, the combination does not explicitly show performing a protocol translation between the targeted device and the common gateway interface, and wherein the translation occurs between a short range communication protocol and a wireless access protocol.

Marchand shows performing a protocol translation, wherein the translation occurs between a short range communication protocol and a wireless access protocol (see p. 7, lines 8-25). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the combination with the protocol translation taught by Marchand in order to improve the variety of protocols with which the devices can communicate.

Regarding claim 68, the combination does not explicitly show performing a protocol translation between the targeted device and the common gateway interface, and wherein the translation occurs between a short range communication protocol and a wireless access protocol.

Marchand shows performing a protocol translation, wherein the translation occurs between a short range communication protocol and a wireless access protocol (see p. 7, lines 8-25). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the combination with the protocol translation taught by Marchand in order to improve the variety of protocols with which the devices can communicate.

**Claims 54, 56, 63, and 69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nielsen (US Pub. No. 2002/0180582) in view of White (US Patent No. 6,049,877), and further in view of Huang (“Pervasive Computing: What Is It Good For?”).**

Regarding claim 54, the combination does not explicitly show wirelessly connecting between the mobile terminal and another targeted device being a home appliance maintaining a list of items, and automatically downloading the item list and formatting a shopping list via the common gateway interface.

Huang shows connecting between a mobile terminal and a targeted device begin a home appliance maintaining a list of items (comprising a refrigerator maintaining a shopping list), and automatically downloading the item list and formatting a shopping list (comprising downloading the shopping list to a PDA: see sections 1.1 and 1.2 on p. 85). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the combination with the automated home appliance taught by Huang in order to make grocery shopping more convenient for the user.

Regarding claim 56, the combination further shows wherein the home appliance is a refrigerator that maintains a list of edible items (see Huang, sections 1.1 and 1.2 on p. 85).

Regarding claim 63, the combination does not explicitly show wirelessly connecting between the mobile terminal and another targeted device being a home appliance maintaining a

list of items, and automatically downloading the item list and formatting a shopping list via the common gateway interface.

Huang shows connecting between a mobile terminal and a targeted device begin a home appliance maintaining a list of items (comprising a refrigerator maintaining a shopping list), and automatically downloading the item list and formatting a shopping list independently of human interaction (comprising downloading the shopping list to a PDA: see sections 1.1 and 1.2 on p. 85). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the combination with the automated home appliance taught by Huang in order to make grocery shopping more convenient for the user.

Regarding claim 69, the combination does not explicitly show wirelessly connecting between the mobile terminal and another targeted device being a home appliance maintaining a list of items, and automatically downloading the item list and formatting a shopping list via the common gateway interface.

Huang shows connecting between a mobile terminal and a targeted device begin a home appliance maintaining a list of items (comprising a refrigerator maintaining a shopping list), and automatically downloading the item list and formatting a shopping list independently of human interaction (comprising downloading the shopping list to a PDA: see sections 1.1 and 1.2 on p. 85). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the combination with the automated home appliance taught by Huang in order to make grocery shopping more convenient for the user.

**Claims 55, 64, and 70 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nielsen (US Pub. No. 2002/0180582) in view of White (US Patent No. 6,049,877), and further in view of Carcerano (US Patent No. 6,308,205).**

Regarding claim 55, the combination does not explicitly show wirelessly connecting between the mobile terminal and another targeted one of the wirelessly connected proximate devices; causing, at least in part, receiving via the common gateway interface current configuration of the other targeted device; and causing, at least in part, transmitting via the common gateway interface updated configuration of the other targeted device.

Carcerano shows wirelessly connecting between a terminal and a device (see col. 5, lines 25-30); and receiving, via a common gateway interface current configuration of the other device (see col. 13, lines 5-16 and Figs. 5 and 7); and transmit via the common gateway interface updated configuration of the other targeted device (see col. 13, lines 5-16). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the combination to use the configuration management of Carcerano in order to allow users to remotely administer devices.

Regarding claim 64, the combination does not explicitly show wirelessly connecting between the mobile terminal and another targeted one of the wirelessly connected proximate devices; causing, at least in part, receiving via the common gateway interface current configuration of the other targeted device; and causing, at least in part, transmitting via the common gateway interface updated configuration of the other targeted device.

Carcerano shows wirelessly connecting between a terminal and a device (see col. 5, lines 25-30); and receiving, via a common gateway interface current configuration of the other device (see col. 13, lines 5-16 and Figs. 5 and 7); and transmit via the common gateway interface updated configuration of the other targeted device (see col. 13, lines 5-16). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the combination to use the configuration management of Carcerano in order to allow users to remotely administer devices.

Regarding claim 70, the combination does not explicitly show wirelessly connecting between the mobile terminal and another targeted one of the wirelessly connected proximate devices; causing, at least in part, receiving via the common gateway interface current configuration of the other targeted device; and causing, at least in part, transmitting via the common gateway interface updated configuration of the other targeted device.

Carcerano shows wirelessly connecting between a terminal and a device (see col. 5, lines 25-30); and receiving, via a common gateway interface current configuration of the other device (see col. 13, lines 5-16 and Figs. 5 and 7); and transmit via the common gateway interface updated configuration of the other targeted device (see col. 13, lines 5-16). It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the combination to use the configuration management of Carcerano in order to allow users to remotely administer devices.

## Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER D. BIAGINI whose telephone number is (571)272-9743. The examiner can normally be reached on weekdays from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christopher Biagini  
(571) 272-9743

/Andrew Caldwell/  
Supervisory Patent Examiner, Art Unit 2445